(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09062596 A**

(43) Date of publication of application: **07.03.97**

(51) Int. Cl **G06F 13/00**
G09C 1/00
G09C 1/00
G09C 1/00
H04L 9/32
H04L 12/54
H04L 12/58

(21) Application number: **07217678**

(22) Date of filing: **25.08.95**

(71) Applicant: **HITACHI LTD**

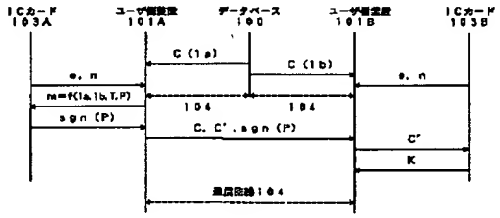
(72) Inventor: **NISHIOKA GENJI**

(54) **ELECTRONIC MAIL SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To improve the security related to transmission/reception of electronic mails.

SOLUTION: This system consists of a data base 100 where the public key of each user is registered, at least two information processors 101a and 101b, and IC cards 103a and 103b. Secret keys of users carrying IC cards 103a and 103b and the public key of an authenticating station are stored in memories of IC cards 103a and 103b. In a transmission source A (information processor 101a), its own secret key stored in the memory is used in the IC card 103a to generate a digital signature for transmission data which includes mail data P, user information Ia for discrimination of the transmission source A, user information for discrimination of a transmission destination B, and time information T specifying the transmission date. In a reception side B (information processor 101b), the transmission source, the destination, and the generation date of the electronic mail are verified based on the digital signature included in the received electronic mail.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－62596

(43)公開日　平成９年(1997)３月７日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　13/00	３５１		Ｇ０６Ｆ　13/00	３５１Ｇ	
Ｇ０９Ｃ　1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６３０Ｄ	
		7259－5Ｊ		６３０Ｆ	
	６４０	7259－5Ｊ		６４０Ｂ	
	６６０	7259－5Ｊ		６６０Ａ	

審査請求　未請求　請求項の数19　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平7－217678

(22)出願日　平成７年(1995)８月25日

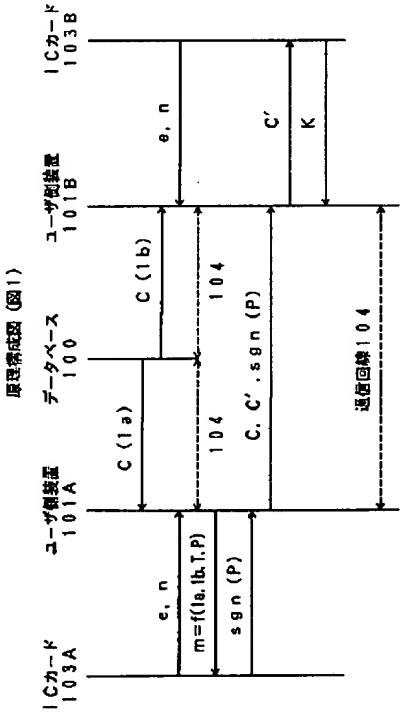
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　西岡　玄次
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

(54)【発明の名称】　電子メールシステム

(57)【要約】
【目的】電子メールの送受信に関するセキュリティの向上を図る。
【構成】本システムは、各ユーザの公開鍵が登録されたデータベース１００と少なくとも２台の情報処理装置１０１ａ，１０１ｂとＩＣカード１０３ａ，１０３ｂから構築される。各ＩＣカード１０３ａ，１０３ｂのメモリにはこれを所持するユーザの秘密鍵と認証局の公開鍵が格納されている。送信元Ａ（情報処理装置１０１ａ）では、ＩＣカード１０３ａの内部で、メモリに格納された自己の秘密鍵を用いて、メールデータＰと送信元Ａを識別するためのユーザ情報Ｉａと送信先Ｂを識別するためのユーザ情報と送信日時を特定する時間情報Ｔとを含む送信データに対するデジタル署名を作成する。受信側Ｂ（情報処理装置１０１ｂ）は、受信した電子メールに含まれるデジタル署名を基に、電子メールの送信元、宛先、作成日時を検証する。



1

【特許請求の範囲】

【請求項１】送信元の秘密鍵によりデジタル署名を作成する作成手段と、前記作成手段が作成したデジタル署名を、送信する電子メールのメールデータに付加して送信する送信手段とを備える電子メール送信装置であって、前記作成手段は、前記送信元の公開鍵で前記電子メールの送信元と送信先とを検証できるように、前記送信元の秘密鍵により、前記送信元で作成されたメールデータと前記送信元を特定するユーザ情報と前記電子メールの送信先を特定するユーザ情報とを含んだ情報に対して、前記デジタル署名を作成することを特徴とする電子メール送信装置。

【請求項２】請求項１記載の電子メール送信装置であって、

前記電子メールを複数の送信先に対して送信する場合、前記作成手段は、前記送信元で作成されたメールデータと、前記送信元を特定するユーザ情報と、前記各送信先を特定する複数のユーザ情報とを含んだ情報に対して、前記デジタル署名を作成することを特徴とする電子メール送信装置。

【請求項３】請求項１または２記載の電子メール送信装置であって、

前記作成手段は、

前記情報に含まれるメールデータと各ユーザ情報とを連接した連接データを作成する連接手段と、

前記連接手段が作成した連接データをハッシュ関数に従って圧縮するハッシュ計算手段と、

前記ハッシュ計算手段が圧縮した連接データに対して、前記デジタル署名を作成するデジタル署名作成手段とを備えることを特徴とする電子メール送信装置。

【請求項４】請求項１または２記載の電子メール送信装置であって、

前記情報は、更に、前記デジタル署名により前記電子メールの送信日時を検証できるように、前記電子メールの送信日時を特定する時間情報を含むことを特徴とする電子メール送信装置。

【請求項５】請求項４記載の電子メール送信装置であって、

前記作成手段は、

前記情報に含まれるメールデータと各ユーザ情報と前記電子メールの送信日時を特定する時間情報とを連接した連接データを作成する連接手段と、

前記連接手段が作成した連接データをハッシュ関数に従って圧縮するハッシュ計算手段と、

前記ハッシュ計算手段が圧縮した連接データに対して、前記デジタル署名を作成するデジタル署名作成手段を備えることを特徴とする電子メール送信装置。

【請求項６】請求項３、４または５記載の電子メール送信装置であって、

電子メール送信装置は、

2

前記送信手段と、前記連接手段と、前記ハッシュ計算手段とを含んだ本体装置と、

前記送信元のパスワードで暗号化した送信元の秘密鍵の暗号文を記憶するメモリと、前記メモリに記憶された秘密鍵の暗号文を送信元のパスワードで復号する復号手段と、前記デジタル署名作成手段とを内蔵する、前記本体装置に着脱可能なＩＣカードとにより構成され、

前記デジタル署名作成手段は、前記復号手段で複合された送信元の秘密鍵により、前記デジタル署名を作成することを特徴とする電子メール送信装置。

【請求項７】送信元の秘密鍵により作成されたデジタル署名を含む電子メールを受信する電子メール受信装置であって、

前記電子メールは、前記電子メールの送信元で作成されたメールデータと前記送信元を特定するユーザ情報と前記電子メールの１以上の送信先を特定するユーザ情報とを含んだ情報に対して作成されたデジタル署名を含み、

当該電子メール受信装置は、

前記デジタル署名と前記送信元の公開鍵とにより、前記電子メールの送信元と送信先とを検証する検証手段を備えることを特徴とする電子メール受信装置。

【請求項８】請求項７記載の電子メール受信装置であって、

前記電子メールは、送信日時を特定する時間情報を加えた情報に対して作成されたデジタル署名を含み、

前記検証手段は、前記デジタル署名と前記送信元の公開鍵とにより、更に、前記電子メールの送信日時を検証することを特徴とする電子メール受信装置。

【請求項９】請求項１、２、または３記載の電子メール送信装置と、

請求項７記載の電子メール受信装置とを備えることを特徴とする電子メールシステム。

【請求項１０】請求項４または５記載の電子メール送信装置と、

請求項８記載の電子メール受信装置とを備えることを特徴とする電子メールシステム。

【請求項１１】請求項９または１０記載の電子メールシステムであって、

前記電子メール送信装置は、

前記送信手段と前記連接手段と前記ハッシュ計算手段とを含む本体装置と、

前記本体装置に着脱可能なＩＣカードとから構成され、

前記電子メール受信装置は、

前記検証手段を含む本体装置と、

前記本体装置に着脱可能なＩＣカードとから構成され、

当該電子メールシステムは、

前記電子メール送信装置のＩＣカードと前記電子メール受信装置のＩＣカードを作成すると共に、自身の秘密鍵で暗号化したユーザの公開鍵の暗号文を登録したデータベースを有するデータベースサーバを備えた認証局を備

え、
前記電子メール受信装置のＩＣカードと前記電子メール送信装置のＩＣカードは、それぞれ、
前記ＩＣカードのユーザのパスワードで暗号化された前記ＩＣカードのユーザの秘密鍵の暗号文と、前記認証局の公開鍵とを記憶するメモリと、
前記メモリに記憶された認証局の公開鍵で、前記認証局のデータベースサーバのデータベースに登録された前記ＩＣカードのユーザの公開鍵の暗号文を復号する公開鍵復号手段と、
前記ＩＣカードのユーザから入力された前記ＩＣカードのユーザのパスワードで、前記メモリに格納された秘密鍵の暗号文を復号する秘密鍵復号手段とを内蔵することを特徴とする電子メールシステム。
【請求項１２】自身の秘密鍵で暗号化した、ユーザの公開鍵を含む情報の暗号文を、ユーザの要求に応じてユーザに報告する認証局を備える電子メールシステムにおいて、前記認証局の公開鍵を管理する鍵管理方法であって、
前記認証局が、前記認証局の公開鍵と前記ユーザのパスワードで暗号化された前記ユーザの秘密鍵の暗号文とを格納したメモリと、入力された前記ユーザのパスワードで前記メモリに格納された秘密鍵の暗号文を復号する第一の復号手段とを内蔵するＩＣカードを作成するステップと、
前記ユーザの秘密鍵の正当性を検証できるように、前記ＩＣカードに対する前記ユーザの操作に応じて、前記第一の復号手段が、入力された前記ユーザのパスワードで前記メモリに格納された前記ユーザの秘密鍵の暗号文を復号した前記ユーザの秘密鍵を出力するステップとを有することを特徴とする鍵管理方法。
【請求項１３】自身の秘密鍵で暗号化した、ユーザの公開鍵を含む情報の暗号文を、ユーザの要求に応じてユーザに報告する認証局を備える電子メールシステムにおいて、前記認証局の公開鍵を管理する鍵管理方法であって、
前記認証局は、受付けた各ユーザの公開鍵の暗号文を含むユーザ情報を登録するデータベースを有するデータベースサーバを備え、

当該鍵管理方法は、
前記認証局が、前記認証局の公開鍵と前記ユーザのパスワードで暗号化された前記ユーザの秘密鍵の暗号文とを格納したメモリと、入力された前記ユーザのパスワードで前記メモリに格納された秘密鍵の暗号文を復号する第一の復号手段と、前記メモリに格納された認証局の公開鍵で前記データベースに登録された前記ユーザの公開鍵の暗号文を復号する第二の鍵復号手段とを内蔵するＩＣカードを作成すると共に、前記認証局の秘密鍵で暗号化した前記ユーザ情報の暗号文を前記データベースサーバのデータベースに登録するステップと、
前記ユーザの秘密鍵の正当性を検証できるように、前記ＩＣカードに対する前記ユーザの操作に応じて、入力された前記ユーザのパスワードで、前記第一の復号手段が、前記メモリに格納された前記ユーザの秘密鍵の暗号文を復号した前記ユーザの秘密鍵を出力するステップと、
前記ユーザの公開鍵の正当性を検証できるように、前記第二の復号手段が、前記メモリに格納された認証局の公開鍵で前記データベースに登録された前記ユーザの公開鍵の暗号文を復号した前記ユーザの公開鍵を出力するステップとを有することを特徴とする鍵管理方法。
【請求項１４】請求項３記載の電子メール送信装置であって、
前記連接手段は、前記メールデータＰと、前記各ユーザ情報とを連接した連接データｍを作成し、
前記ハッシュ計算手段は、前記連接データｍをハッシュ関数ｆに従って、
【数１】

$$m_1 = f\ (m) \qquad \cdots \text{数式 1}$$

により圧縮した圧縮データm_1を作成し、
前記デジタル署名作成手段は、前記送信元の秘密鍵とd_1と公開鍵（e_1，n_1）とで、前記ハッシュ計算手段が作成した圧縮データm_1に対して、
【数２】

$$sgn\ (P) = m_1^{e_1} \pmod{n_1} \qquad \cdots \text{数式 2}$$

により前記デジタル署名ｓｇｎ（Ｐ）を作成し、
前記送信手段は、
前記作成手段が作成したデジタル署名ｓｇｎ（Ｐ）と、ランダムに作成されたデータ暗号化鍵Ｋで、
【数３】

$$C_1 = E\ (K : P) \qquad \cdots \text{数式 3}$$

により暗号化されたメールデータＰの暗号文C_1と、
前記送信先の公開鍵（e_2，n_2）で、
【数４】

$$C_2 = K^{e_2} \pmod{n_2} \qquad \cdots \text{数式 4}$$

により暗号化された前記データ暗号化鍵Ｋの暗号文C_2とを含んだ前記電子メールを、前記送信先に送信することを特徴とする電子メール送信装置。
【請求項１５】請求項１４記載の電子メール送信装置であって、
前記送信する電子メールは、更に、前記電子メールの送

5

信日時を特定する時間情報Ｔを含み、
前記情報は、更に、前記デジタル署名ｓｇｎ（Ｐ）により前記電子メールの送信日時を検証できるように、前記電子メールの送信日時を特定する時間情報Ｔを含み、
前記連接手段は、前記情報に含まれる前記メールデータＰと各ユーザ情報と前記時間情報Ｔとを連接した連接データｍを作成することを特徴とする電子メール送信装置。
【請求項１６】請求項７記載の電子メール受信装置であって、
前記受信した電子メールは、
ランダムに作成されたデータ暗号化鍵Ｋで、
【数５】

$$C_1 = E\ (K : P) \qquad \cdots 数式5$$

により暗号化されたメールデータＰの暗号文C_1と、
前記送信先の公開鍵（e_2, n_2）で、
【数６】

$$C_2 = K^{e_2} \bmod n_2 \qquad \cdots 数式6$$

により暗号化されたデータ暗号化鍵Ｋの暗号文C_2と、
前記送信元を特定するユーザ情報と前記電子メールの１以上の送信先を特定するユーザ情報とメールデータＰを含んだ情報に対して作成されたデジタル署名ｓｇｎ（Ｐ）とを含み、

$$K = C_2^{d_2} \bmod n_2 \qquad \cdots 数式7$$

により復号する第一の復号手段と、
前記受信した電子メールに含まれる前記メールデータＰの暗号文C_1を、第一の復号手段で復号された前記データ暗号化鍵Ｋで、
【数８】

$$P = D\ (K : C_1) \qquad \cdots 数式8$$

により復号する第二の復号手段と、
前記第二の復号手段で復号されたメールデータＰと各ユ

$$f\ (m) \equiv sgn\ (P)^{e_1} \quad (\bmod\ n_1) \qquad \cdots 数式9$$

により検証することを特徴とする電子メール受信装置。
【請求項１７】請求項１６記載の電子メール受信装置であって、
前記受信した電子メールは、前記デジタル署名により前記電子メールの送信日時を検証できるように、更に前記電子メールの送信日時を特定する時間情報Ｔを含んだ情報に対して作成されたデジタル署名を含むと共に、更に、前記受信した電子メールの送信日時を特定する時間情報Ｔを含み、
前記連接手段は、前記電子メールのメールデータＰと各ユーザ情報と時間情報Ｔを連接した連接データｍを作成することを特徴とする電子メール受信装置。
【請求項１８】請求項１４記載の電子メール送信装置と、
請求項１６記載の電子メール受信装置とを備えることを特徴とする電子メールシステム。
【請求項１９】請求項１５記載の電子メール送信装置と、
請求項１７記載の電子メール受信装置とを備えることを特徴とする電子メールシステム。
【発明の詳細な説明】

6

って、
前記受信した電子メールは、
ランダムに作成されたデータ暗号化鍵Ｋで、
【数５】

$$C_1 = E\ (K : P) \qquad \cdots 数式5$$

により暗号化されたメールデータＰの暗号文C_1と、
前記送信先の公開鍵（e_2, n_2）で、
【数６】

$$C_2 = K^{e_2} \bmod n_2 \qquad \cdots 数式6$$

当該電子メール受信装置は、
前記受信した電子メールに含まれる前記データ暗号化鍵Ｋの暗号文C_2を、前記送信先の秘密鍵d_2と公開鍵（e_2, n_2）とで、
【数７】

$$K = C_2^{d_2} \bmod n_2 \qquad \cdots 数式7$$

ーザ情報とを連接した連接データｍを作成する連接手段とを備え、
前記検証手段は、前記受信した電子メールの送信元と送信先とを、前記受信した電子メールに含まれるデジタル署名ｓｇｎ（Ｐ）と、前記連接手段が作成した連接データｍと、ハッシュ関数ｆと、送信元の公開鍵（e_1, n_1）で、
【数９】

$$f\ (m) \equiv sgn\ (P)^{e_1} \quad (\bmod\ n_1) \qquad \cdots 数式9$$

【０００１】
【産業上の利用分野】本発明は、電子メールの送受信に関するセキュリティを管理する電子メール暗号システムに関する。
【０００２】
【従来の技術】Ｉｎｔｅｒｎｅｔでの電子メールの送受信に関するセキュリティを管理するための方法として、Ｌｉｎｎ，Ｊ．，ｅｔ，ａｌ，Ｐｒｉｖａｃｙ Ｅｎｈａｎｃｅｍｅｎｔ Ｍａｉｌ ｆｏｒ Ｉｎｔｅｒｎｅｔ Ｅｌｅｃｔｒｏｎｉｃ Ｍａｉｌ：Ｐａｒｔ Ｉ，ＩＩ，ＩＩＩ，ＩＶ，ＲＥＦ－１４２１－１４２４，１９９３記載のＰＥＭ（Ｐｒｉｖａｃｙ Ｅｎｈａｎｃｅｍｅｎｔ Ｍａｉｌ）が知られている。これは、米国内務省標準局により標準の暗号化方式として公表されたＤＥＳで暗号化したメールデータに、ＲＳＡに基づいて作成した送信元を識別するためのデジタル署名を付与することにより、電子メールの送受信に関するセキュリティの向上を図るものである。以下、この詳細について説明する。なお、ＲＳＡについてはＲ．Ｌ．Ｒｉｖｅｓｔ，Ａ．Ｓｈａｍｉｒ，Ｌ．Ａｄｌｅｍａｎ，．Ａ Ｍｅｔｈｏｄ ｆｏｒ Ｏｂｔａｉｎｉｎｇ Ｄｉｇｉｔａｌ

7

Sigunatures and Public Key Cryptosysytems, Comuunications of The ACM, Vol. 21, 1978に、また、DESについてはData Encryption Standard, FIPS－PUB－46, 19773に、各々、詳細が記載されている。

【0003】最初に、PEMによる管理下における、電子メールの送受信に関する一連の処理（後述）において使用される公開鍵（e, n）について説明する。

【0004】PEMを利用する各ユーザには、それぞれ、公開鍵（e, n）が割り当てられている。そして、PEMの正当な各ユーザには、認証局固有の公開鍵（e', n'）が正当な手段により教示される。また、こうしたユーザには、それぞれ、そのユーザの公開鍵（e, n）等の、PEMによる管理下において電子メールの送受信を行うために必要とされる情報を認証局の秘密鍵d'で暗号化した暗号文が記載された公開鍵証明書が、一種の身分証明書として発行される。

【0005】次に、このような公開鍵（e, n）を利用した、PEMの管理下における、電子メールの送受信に関する一連の処理について説明する。ただし、電子メールの送信元Aと送信先Bは、正当な手段により認証局に登録されたユーザ同士であり、事前に、互いに相手の公開鍵証明書を正当な手段（例えば、互いに公開鍵証明書を送付し合う等）で獲得していることを前提とする。

【0006】まず、電子メールの送信元Aでの処理について説明する。

$$sgn_1(P) = f(P)^{e_1} \pmod{n_1} \quad \cdots \text{数式12}$$

【0014】ここで、f（P）は、データを圧縮するハッシュ関数である。なお、このハッシュ関数fは、PEMの管理下において、一般に公開される情報に含まれる関数である。

【0015】ここまでの処理が完了したら、送信元Aは、送信先Bへ、C_1, C_2, sgn_1（P）を電子メールとして送信する。

【0016】次に、この電子メールの送信先Bにおいて電子メールが受信された場合の処理について説明する。ただし、電子メールを受信した後から、送信先Bを受信側Bと呼び替えるものとする。

【0017】送信先Bにおいて送信元Aからの電子メールが受信されると、受信側Bでは、まず、自身Bの公開鍵（e_2, n_2）と秘密鍵d_2を併用して、数式13に基づく処理を施すことにより、受信した電子メールに含まれるC_2を復号してデータ暗号化鍵Kを得た後、更に、このデータ暗号化鍵Kを使用して、数式14に基づく処理を施すことにより、電子メールに含まれるC_1を復号してメールデータPを得る。

【0018】

8

【0007】さて、送信元Aでは、まず、作成したメールデータPを暗号化するためのデータ暗号化鍵Kを任意に作成する。そして、この鍵暗号Kを使用し、次式に基づいて、DESによる暗号化処理をメールデータPに対して施すことにより、メールデータの暗号文C_1を作成する。

【0008】

【数10】

$$C_1 = E(K : P) \quad \cdots \text{数式10}$$

【0009】ここで、E（K：P）は、鍵暗号Kでメールデータを暗号化するための関数である。

【0010】また、認証局の公開鍵（e', n'）を使用して、事前に獲得しておいた送信先Bの公開鍵証明書に記載された暗号文から送信先Bの公開鍵（e_2, n_2）を復号する。更に、得られた送信先Bの公開鍵（e_2, n_2）を使用して、次式に基づくRSAによる暗号化処理をデータ暗号化鍵Kに施すことにより、データ暗号化鍵Kの暗号文C_2を作成する。

【0011】

【数11】

$$C_2 = K^{e_2} \pmod{n_2} \quad \cdots \text{数式11}$$

【0012】そして、送信元Aは、自身の秘密鍵d_1と公開鍵（e_1, n_1）とを併用し、メールデータPの作成者が自身であることを証明するためのデジタル署名sgn_1（P）を次式に基づいて作成する。

【0013】

【数12】

$$sgn_1(P) = f(P)^{e_1} \pmod{n_1} \quad \cdots \text{数式12}$$

【数13】

$$K = C_2^{d_2} \pmod{n_2} \quad \cdots \text{数式13}$$

【0019】

【数14】

$$P = D(K : C_1) \quad \cdots \text{数式14}$$

【0020】ここで、D（K：C_1）は、データ暗号化鍵Kで、電子メールに含まれるC_1を復号する関数である。

【0021】そして、このメールデータPの作成者と電子メールの送信元とが同一であることを検証するため、すなわち、電子メールに含まれたデジタル署名sgn_1（P）が確かに電子メールの送信元Aにより作成されたものであることを検証するために、数式14により得られたメールデータPと、電子メールの送信元Aの公開鍵（e_1, n_1）とが次式の関係を満足することを確認する。万が一、数式14により得られたメールデータPと、電子メールの送信元Aの公開鍵（e_1, n_1）とが次式の関係を満足しないならば、メールデータPの作成者

とこの電子メールの送信元とが異なるユーザであることになり、何者かによりメールデータＰが不当に改竄されている可能性を疑う必要がある。

【００２２】

【数１５】

$$f(P) \equiv sgn_1(P)^{e_1} \pmod{n_1} \quad \cdots \text{数式１５}$$

【００２３】なお、ここで使用する電子メールの送信元Ａの公開鍵（e_1, n_1）は、認証局の公開鍵（e', n'）を使用して、送信元Ａの公開鍵証明書に記載された暗号文を復号することにより得られたものである。

【００２４】このように、ＰＥＭによる管理下で電子メールの送受信を行えば、盗聴や内容改竄等の不正な行為を防止することができる。

【００２５】

【発明が解決しようとする課題】ところが、上記ＰＥＭでは、電子メールの送信元Ａにおいてメールデータ Ｐの作成者を識別するためのデジタル署名 sgn_1（Ｐ）は付与されるけれども、メールデータＰがいづれのユーザに宛てて作成されたものであるかを識別するための情報は付与されないため、電子メールの受信側Ｂにおいては、受信した電子メールに含まれているメールデータＰが、確かに自身に宛て作成されたものであるということの確証をつかむことができない。すなわち、メールデータの内容が改竄されていなければ、同一の作成者により作成された別のメールデータによって、メールデータの内容がすり替えられていても、受信側ではこれを検知できないという問題があった。例えば、電子メールの受信側Ｂが、受信した電子メール（何らかの提案Ｃに対して賛否を問う内容のメールデータ）に対する応答文Ｐ（賛成である旨を記載したもの）を作成し、これにデジタル署名 sgn_1（Ｐ）を付与して、送信先Ａに電子メールとして返送した場合に、不正者が、誤った情報を流す目的をもって、以前にＢから送信されたデジタル署名付きの電子メールのメールデータの内から、応答文として悪用できる内容のメールデータ P_1（反対である旨を記載したもの）を不正に使用して、電子メールのメールデータのすり替えを行っても、これを受信したＡでは、メールデータ P_1 に付与されたデジタル署名 sgn_1（P_1）により、確かにＢからの応答文であることを確認して、その内容を信頼することになる。

【００２６】また、上記ＰＥＭによる管理下では、個々のユーザの公開鍵については、認証局が発行した公開鍵証明書によってそれが正当なものであることが証明されるが、認証局自体の公開鍵については、個々のユーザ側からそれが正当なものであるかどうかを確認することができない。こうしたことが、ＰＥＭを利用するユーザが、不正なユーザの不正行為による被害を被る原因となる可能性は高い。例えば、不正なユーザが、認証局の公開鍵を偽って、認証局になりすますという可能性がある。

【００２７】そこで、本発明は、電子メールの送受信に関するセキュリティの向上を図るために適した電子メール暗号システムを提供することを目的とする。

【００２８】

【課題を解決するための手段】上記目的達成のために、本発明は、送信元の秘密鍵によりデジタル署名を作成する作成手段と、前記作成手段が作成したデジタル署名を、送信する電子メールのメールデータに付加して送信する送信手段とを備える電子メール送信装置であって、前記作成手段は、前記送信元の公開鍵で前記電子メールの送信元と送信先とを検証できるように、前記送信元の秘密鍵により、前記送信元で作成されたメールデータと前記送信元を特定するユーザ情報と前記電子メールの送信先を特定するユーザ情報とを含んだ情報に対して、前記デジタル署名を作成することを特徴とする電子メール送信装置を提供する。

【００２９】更に、送信元の秘密鍵により作成されたデジタル署名を含む電子メールを受信する電子メール受信装置であって、前記電子メールは、前記電子メールの送信元で作成されたメールデータと前記送信元を特定するユーザ情報と前記電子メールの１以上の送信先を特定するユーザ情報とを含んだ情報に対して作成されたデジタル署名を含み、当該電子メール受信装置は、前記デジタル署名と前記送信元の公開鍵とにより、前記電子メールの送信元と送信先とを検証する検証手段を備えることを特徴とする電子メール受信装置を提供する。

【００３０】そして、こうした電子メール送信装置と電子メール受信装置とを備えた電子メールシステムを提供する。

【００３１】

【作用】本発明に係る電子メール送信装置によれば、前記作成手段は、前記送信元で作成されたメールデータと前記送信元を特定するユーザ情報と前記電子メールの送信先を特定するユーザ情報とを含んだ情報に対して、前記送信元の公開鍵で前記電子メールの送信元と送信先との検証が可能な前記デジタル署名を作成する。

【００３２】また、本発明に係る電子メール受信装置によれば、前記検証手段は、前記受信した電子メールに含まれるデジタル署名と、前記送信元の公開鍵とにより、前記電子メールの送信元と送信先とを検証する。

【００３３】そして、本発明に係る電子メールシステムは、こうした電子メール送信装置と電子メール受信装置とから構築されるので、電子メール受信装置側では、前記電子メール送信装置側で付与されたデジタル署名により、受信した電子メールの送信元と宛先とを確認することができる。従って、不正なユーザによるメールデータ

のすり替え等を防止することができる。その結果、各装置の間で送受信される電子メールの機密性が保持される。

【００３４】また、電子メールシステムの構成として、各ユーザの公開鍵の暗号文を含むユーザ情報を登録するデータベースを有するデータベースサーバを備えた認証局を加えて、この認証局により各ユーザの公開鍵を一元的に管理するようにすれば、従来ＰＥＭにおいて不明確であった認証局の公開鍵の正当性を容易に確認することができる。すなわち、認証局は、各ユーザから受付けた、各ユーザの公開鍵を含むユーザ情報を、自身の秘密鍵で暗号化してデータベースに登録すると共に、認証局の公開鍵を格納したメモリを内蔵するＩＣカードを作成する。一方、認証局からＩＣカードを受け取った各ユーザは、認証局のデータベースにアクセスして自身のユーザ情報の暗号文を取得することにより、まず、自身が、本システムを利用するユーザとして正式に登録されているかを確認する。更に、ＩＣカードのメモリに格納された認証局の公開鍵で、認証局のデータベースにアクセスして取得した自身のユーザ情報の暗号文を復号し、このユーザ情報に含まれる公開鍵の正当性を確認する。このとき、万一、このユーザ情報に含まれる公開鍵の正当性が確認できなければ、ユーザの登録の段階で認証局のなりすまし等の不正が行われたことが裏付けられたことになる。このように認証局のデータベースによって各ユーザの公開鍵を一元的に管理し、かつ、ＩＣカードにより認証局の公開鍵の安全性を確保するようにすれば、認証局の公開鍵の正当性が保証され、システム全体のセキュリティが確保される。

【００３５】更に、このＩＣカードのメモリにユーザの秘密鍵を格納すると共に、このＩＣカードの内部で、ユーザの秘密鍵を用いるデジタル署名を作成する際の処理の実行を可能とすれば、ユーザの秘密鍵の機密性も同時に保持することができるので、システム全体のセキュリティを一層向上させることができる。

【００３６】

【実施例】以下、添付の図面を参照しながら、本発明に係る実施例について説明する。

【００３７】まず、図１を参照しながら、本実施例に係るシステムの基本的な構成について説明する。以下、秘密鍵暗号方式としてＤＥＳを用いる場合を一例に挙げて説明するが、本システムにおける秘密鍵暗号方式は、必ずしもこれである必要はない。例えば、ＦＥＡＬ等の、他の方式を用いても構わない。

【００３８】本システムは、図１に示すように、従来技術の欄で説明した認証局に相当する情報処理装置１００と、少なくとも２台の情報処理装置１０１ａ，１０１ｂと、メールデータに付与するデジタル署名の作成処理等を行なうＩＣカード１０３ａ，１０３ｂとにより構築される。ただし、２台の情報処理装置１０１ａ，１０１ｂの間と、各報処理装置１００，１０１ａ，１０１ｂの間は、相互にデータの転送が行なえるように、各々通信回線１０４で接続されている。また、各情報処理装置１０１ａ，１０１ｂは、装着したＩＣカード１０３ａ，１０３ｂとの間で、相互にデータの入出力を行なうことができる。

【００３９】これらの情報処理装置１０１ａ，１０１ｂは、それぞれ、図２に示すように、作成したメールデータ等を表示する表示装置２０１ａ，２０１ｂと、ＩＣカード１０３ａ，１０３ｂ用のＩ／Ｏポート２０２ａ，２０２ｂと、ＲＳＡによる暗号処理を行なうＲＳＡ暗号処理部２０３ａ，２０３ｂと、ＤＥＳによる暗号処理を行なうＤＥＳ暗号処理部２０４ａ，２０４ｂと、メモリ２０５ａ，２０５ｂと、乱数を発生する乱数発生部２０６ａ，２０６ｂと、乱数発生部２０６ａ，２０６ｂが発生する乱数から鍵暗号Ｋを作成する鍵生成部２０７ａ，２０７ｂと、ハッシュ関数によりデータを圧縮するハッシュ計算部２０８ａ，２０８ｂと、メールデータに付与されたデジタル署名を検証するデジタル署名検証部２０９ａ，２０９ｂと、通信回線１０４で相互に接続された他の情報処理装置との間の通信の制御する通信制御部２１０ａ，２１０ｂと、メールデータ等を入力する入力装置（キーボード等）（不図示）とを備える。そして、これら各ブロック間のデータ転送はバス２１２を介して行なわれる。なお、この構成は、ハードウエアと、ＣＰＵにより実現されるプロセスとを機能的に示したものである。

【００４０】一方、ＩＣカード１０３ａ，１０３ｂは、装着された情報処理装置１０１ａ，１０１ｂからのデータの入力を制御する入力部３０１ａ，３０１ｂと、パスワードｓから鍵暗号化鍵K_1を作成する鍵暗号生成部３０２ａ，３０２ｂと、認証局の公開鍵（ｅ’，ｎ’）等を格納するメモリ３０３ａ，３０２ｂと、ＤＥＳによる暗号処理を行なうＤＥＳ暗号処理部３０４ａ，３０４ｂと、ＲＳＡによる暗号処理を行なうＲＳＡ暗号処理部３０５ａ，３０５ｂと、デジタル署名を作成するデジタル署名作成部３０６ａ，３０６ｂと、装着された情報処理装置１０１ａ，１０１ｂへのデータの出力を制御する出力部３０７ａ，３０７ｂとを備える。なお、この構成は、ハードウエアと、ＣＰＵにより実現されるプロセスとを機能的に示したものである。

【００４１】以上で、本システムの構成についての説明を終わる。

【００４２】次に、このように構築されたシステムの管理下で行なわれる、電子メールの送受信に関する処理について説明する。

【００４３】最初に、ユーザが本システムを利用するための前提として行う、情報処理装置１００のデータベースへの登録処理について説明する。

【００４４】まず、本システムを利用とするユーザは、各々、次式を満足するように、自身の公開鍵（ｅ，ｎ）と

秘密鍵ｄとを任意に作成する。ただし、ｅとｎは整数であり、ｐとｑは、ＲＳＡによる暗号化において機密性が確保される程度に大きな、互いに異なる値を有する素数である。なお、以下、対応する公開鍵と秘密鍵は、全て、これと同様な関係を満足するように作成されたものであることを前提とする。

$$e \cdot d = 1 \mod l.c.d\ (p-1, q-1) \quad \cdots 数式17$$

【００４７】ただし、上式において、ｌ．ｃ．ｄ(ｐ-1,ｑ-1)は、２つの整数ｐ-1,ｑ-1の最小公倍数を意味する。

【００４８】次に、自身のパスワードｓを任意に作成し、これを次式に基づいて暗号化して、鍵暗号化鍵K_1を作成する。

【００４９】

【数１８】

$$K_1 = F(s) \quad \cdots 数式18$$

【００５０】ここで、Ｆ(ｓ)は、従来技術の欄で説明したＰＥＭの管理下において公開される情報に含まれる周知の鍵生成関数である。

【００５１】更に、この鍵暗号化鍵K_1を使用して、次式に基づくＤＥＳによる暗号化処理を秘密鍵ｄに施すことにより、秘密鍵ｄの暗号文Ｃを作成する。

【００５２】

【数１９】

$$C(I_1) = I_1^{d'} \mod n' \quad \cdots 数式20$$

【００５６】さて、こうして情報処理装置１００のデータベースに登録された各ユーザには、それぞれ、自身の秘密鍵d_1の暗号文C_1と認証局の公開鍵(ｅ',ｎ')とが格納されたメモリ３０３を内蔵するＩＣカード１０３が配布される。こうした情報処理装置１００のデータベースへのユーザの登録は、然るべき調査を経た後、信頼のおけるユーザに関してのみ行なわれるものであり、例えば、登録を申請したユーザが自身に関する固有情報を偽る不正な者である場合等には、こうしたユーザは登録対象から除外される。

【００５７】ところで、システムの安全上、登録されたユーザの側では、認証局からＩＣカード１０３が配布された際に、情報処理装置１００のデータベースにアクセスし、取得した自身のユーザ情報の暗号文$C(I_1)$を、配布されたＩＣカード１０３のメモリ３０３に格納された認証局の公開鍵(ｅ',ｎ')で復号して、このユーザ情報I_1に含まれる公開鍵(ｅ,ｎ)が、申請したものと同一であることを確認することが望まれる。こうした確認を行うことによって、本システムを利用するユーザとしての正当性と、ＩＣカード１０３のメモリ３０３に格納された認証局の公開鍵の正当性が共に保証される。また、これと並行して、各ユーザは、配布されたＩＣカード１０３のメモリ３０３に格納された暗号文C_1を自身のパスワードで復号して得られる秘密鍵ｄが、申請したものと同一であることを確認することが望ましい。万一、自身のパスワードによる復号が不可能である場合等には、ＩＣカード１０３がユーザの手に渡るまでの間に認証局のなりすまし等の不正が行われた可能性を疑う必要がある。

【００５８】以上で、情報処理装置１００のデータベースへの登録処理についての説明を終わる。

【００５９】次に、本システムにおける、電子メールの送受信に関する一連の処理について説明する。ただし、電子メールの送信元Ａ(情報処理装置１０１ａ)と送信先Ｂ(情報処理装置１０１ｂ)は、共に、前述した登録処理により、本システムの正当なユーザとして情報処理装置１００のデータベースに登録された者同士であることを前提とする。また、以下に示す電子メールの送信時及び受信時には、各ユーザＡ,Ｂは、既に、情報処理装置１００のデータベースを検索することによって、互いのユーザ情報の暗号文を獲得しているものとする。

【００６０】まず、電子メールの送信元Ａで行なわれる処理について説明するが、図４に示すように、この処理には、情報処理装置１０１ａの備える構成部(図２に示した各ブロック)を利用して行なわれるものと、ＩＣカ

【００４５】

【数１６】

$$n = p \cdot q \quad \cdots 数式16$$

【００４６】

【数１７】

$$C = E(K_1 : d) \quad \cdots 数式19$$

【００５３】以上の処理が終了したら、ユーザは、公開鍵(ｅ,ｎ)と上式とにより作成した秘密鍵ｄの暗号文Ｃとを情報処理装置１００へ転送することにより自身の登録を依頼する。このとき、情報処理装置１００のデータベースに公開鍵(ｅ,ｎ)と共に登録される固有情報(ユーザ名、メールアドレス等)も転送する。

【００５４】一方、これを受け付けた情報処理装置１００側では、認証局の公開鍵(ｅ',ｎ')及び秘密鍵ｄ'を使用して、転送された固有情報及び公開鍵(ｅ,ｎ)と、登録の有効期限等の記録した付加情報とを含むユーザ情報I_1を次式に基づいて暗号化して暗号文$C(I_1)$を作成する。そして、このユーザ情報の暗号文$C(I_1)$をデータベースに登録する。

【００５５】

【数２０】

15

ード１０３ａの備える構成部(図３に示した各ブロック)を利用して行なわれるものとがあるので、以下、これらを別個に説明していく。

【００６１】電子メールの送信元Ａは、情報処理装置１０１ａが備える構成を利用して、以下に示す処理を行なう。

【００６２】電子メールの送信元Ａは、ＩＣカード１０３ａ用のＩ／Ｏポート２０２ａに接続されたＩＣカード１０３ａのメモリ３０３ａに格納された認証局の公開鍵

16

(e', n')を使用して、送信先Ｂのユーザ情報の暗号文Ｃ(Ｉｂ)を復号して送信先Ｂのユーザ情報Ｉｂを得ると共に、自身Ａのユーザ情報の暗号文Ｃ(Ｉａ)を復号して自身Ａのユーザ情報Ｉａを得る。すなわち、情報処理装置１０１ａのＲＳＡ暗号処理部２０３ａにおいて、次式に基づく復号化処理が実行される。

【００６３】

【数２１】

$$Ib = C(Ib)^{e'} mon \quad n' \quad \cdots 数式21$$

【００６４】

【数２２】

$$Ia = C(Ia)^{e'} mon \quad n' \quad \cdots 数式22$$

【００６５】なお、得られたユーザ情報Ｉａ及びＩｂは、この電子メールが送信されるまで間、一旦、メモリ２０５ａに格納される。

【００６６】また、ＤＥＳによる暗号化処理をメールデータＰに施して、メールデータＰの暗号文C_1を作成する。すなわち、鍵生成部２０７ａにおいて、乱数発生部２０６ａが発生する乱数列を利用する、データ暗号化鍵Ｋの作成が実行された後、ＤＥＳ暗号処理部３０４ａにおいて、次式に基づくメールデータＰの暗号化処理が実行される。

【００６７】

【数２３】

$$C = E(K : P) \quad \cdots 数式23$$

【００６８】なお、作成されたメールデータＰの暗号文Ｃは、この電子メールが送信されるまで間、一旦、メモリ２０５ａに格納される。

【００６９】その後、メールデータＰの暗号化に使用したデータ暗号化鍵Ｋを暗号化し、Ｃ'を作成する。すなわち、ＲＳＡ暗号処理部２０３ａにおいて、送信先Ｂのユーザ情報Ｉｂに含まれる公開鍵(e_2, n_2)を使用した、次式に基づくデータ暗号化鍵Ｋの暗号化処理が実行される。

【００７０】

【数２４】

$$C' = K^{e_2} \quad mod \quad n_2 \quad \cdots 数式24$$

【００７１】なお、作成されたＣ'は、この電子メールが送信されるまで間、一旦、メモリ２０５ａに格納される。

【００７２】以上の処理が終了したら、自身Ａのユーザ情報Ｉａと、送信先Ｂのユーザ情報Ｉｂと、作成したメールデータＰと、現在の日時を特定する時間情報Ｔとから、送信データｍを作成する。すなわち、ハッシュ計算部２０８ａにおいて、次式に基づく圧縮処理が実行され、その結果、送信データｍが作成される。ただし、次式において、$z(x_1, \ldots, xn)$は、データ$x_1, \ldots, xn$を相互に連接する連接関数であり、可変個数のデータ$x_1, \ldots, xn$を入力とする。

【００７３】

【数２５】

$$m = f(z(Ia, Ib, P, T)) \quad \cdots 数式25$$

【００７４】このようにハッシュ関数ｆの入力データを連接関数ｚにより与えるのは、ハッシュ関数ｆの入力データ数が仕様により１に限定されているためである。従って、ハッシュ関数ｆの入力データは、必ずしも連接関数ｚにより与える必要はなく、複数のデータを連結することができる他の適当な関数により与えても構わない。ただし、ハッシュ関数に与えられるデータは、一定の処理で、元の複数のデータに分離可能でなければならない。

【００７５】ここまでの処理が終了したら、作成した送信データｍを、Ｉ／Ｏポート２０２ａを介してＩＣカード１０３ａへと転送する。

【００７６】一方、ＩＣカード１０３ａの入力部３０１ａが、情報処理装置１０１ａ側から転送された送信データｍを受付けると、ＩＣカード１０３ａ側では、この送信データｍが一旦メモリ３０３ａに格納された後、以下に示す、デジタル署名の作成処理が開始される。なお、以下、ＩＣカード１０３ａの備える各構成部と情報処理装置１０１ａの備える各構成部との間のデータ転送は、情報処理装置１０１ａの備えるＩＣカード１０３ａ用のＩ／Ｏポート２０２ａと、ＩＣカード１０３ａの備える入力部３０１ａ及び出力部３０７ａを介して行なわれるものとし、送信元Ａからの入力は、こうしたデータ転送径路を利用して情報処理装置１０１ａの入力装置からＩＣカード１０３ａの各構成部に転送されるものとする。

【００７７】ＩＣカード１０３ａの鍵暗号生成部３０２ａにおいて、送信元Ａから入力されたパスワードs_1が暗号化され、鍵暗号化鍵K_1が作成される。すなわち、

鍵暗号生成部３０２ａにおいて、次式に基づく暗号処理が実行される。

【００７８】

【数２６】

$$K_1 = F(s_1) \quad \cdots \text{数式２６}$$

【００７９】ここで、Ｆ(ｓ)は、前述の鍵生成関数である。

【００８０】鍵暗号生成部３０２ａで鍵暗号化鍵K_1が生成されると、ＤＥＳ暗号処理部３０４ａにおいて、メモリ３０３ａに格納された秘密鍵d_1の暗号文Ｃが、秘密鍵d_1に復号される。すなわち、ＤＥＳ暗号処理部３０４ａにおいて、次式に基づく復号処理が実行される。

【００８１】

【数２７】

$$d_1 = D(K_1 : C) \quad \cdots \text{数式２７}$$

【００８２】更に、デジタル署名作成部２０６において、ＤＥＳ暗号処理部３０４ａで復号された秘密鍵d_1と、メモリ３０３ａに格納された公開鍵(e_1, n_1)と、メモリ３０３ａに格納してある送信データｍに対して、デジタル署名$sgn_1(P)$が作成される。すなわち、デジタル署名作成部２０６において、次式に基づく、デジタル署名の作成処理が実行される。

【００８３】

【数２８】

$$sgn_1(P) = m^{d_1} \bmod n_1 \quad \cdots \text{数式２８}$$

【００８４】ここで、ｆ(Ｐ)は、前述のハッシュ関数である。

【００８５】そして、情報処理装置１０１ａへ、デジタル署名作成部２０６で作成されたデジタル署名$sgn_1(P)$が転送されて、ＩＣカード１０３ａ側で行なわれるデジタル署名の作成処理は終了する。

【００８６】さて、情報処理装置１０１ａのＩＣカード１０３ａ用のＩ／Ｏポート２０２ａが、ＩＣカード１０３ａ側から転送されたデジタル署名$sgn_1(P)$を受付けると、情報処理装置１０１ａ側では、このデジタル署名$sgn_1(P)$を、メモリ２０５ａに格納されたＣ，Ｃ’，Ｉａ，Ｉｂと共に、電子メールとして送信する。以上で、電子メールの送信元Ａで行なわれる処理についての説明を終わる。

【００８７】次に、この電子メールが送信先Ｂ(情報処理装置１０１ｂ)で受信された場合に行なわれる処理を、情報処理装置１０１ｂの備える構成部(図２に示した各ブロック)で行なわれるものと、ＩＣカード１０３ｂの備える構成部(図３に示した各ブロック)で行なわれるものとに分割して説明する。ただし、以下、送信先Ｂを受信側Ｂと呼び替えるものとする。

【００８８】電子メールの受信側Ｂ(情報処理装置１０１ｂ)で電子メールが受信されると、情報処理装置１０１ｂ側から、ＩＣカード１０３ｂ側へと、電子メールに含まれる暗号文Ｃが転送される。ＩＣカード１０３ｂの入力部３０１ｂがこれを受け取ると、ＩＣカード１０３ｂ側では、これを一旦メモリ３０３ｂに格納した後、以下に示す処理を実行する。

【００８９】鍵暗号生成部３０２ｂにおいて、受信側Ｂから入力されたパスワードs_2が暗号化されて、鍵暗号化鍵K_2が作成される。すなわち、鍵暗号生成部３０２ｂにおいて、次式に基づく暗号処理が実行される。

【００９０】

【数２９】

$$K_2 = F(s_2) \quad \cdots \text{数式２９}$$

【００９１】ここで、Ｆ(s_2)は、前述の鍵生成関数である。

【００９２】鍵暗号生成部３０２ｂで鍵暗号化鍵K_2が作成されると、ＤＥＳ暗号処理部３０４ｂにおいて、メモリ３０３ｂに格納された秘密鍵d_2の暗号文Ｃ’が復号される。すなわち、ＤＥＳ暗号処理部３０４ｂにおいて、次式に基づく復号処理が実行される。

【００９３】

【数３０】

$$d_2 = D(K_2 : C) \quad \cdots \text{数式３０}$$

【００９４】ＤＥＳ暗号処理部３０４ｂで秘密鍵d_2が得られると、ＲＳＡ暗号処理部３０５ｂにおいて、この秘密鍵d_2と、受信側Ｂの公開鍵(e_2, n_2)とによって、メモリ３０３ｂに格納された暗号文Ｃが復号される。すなわち、ＲＳＡ暗号処理部３０５ｂにおいて次式に基づく復号処理が実行されて、電子メールの送信元Ａがメールデータ Ｐの暗号化に使用したデータ暗号化鍵Ｋが得られる。

【００９５】

【数３１】

$$K = C'^{d_2} \bmod n_2 \quad \cdots \text{数式３１}$$

【００９６】ここまでの処理が終了したら、このデータ暗号化鍵Ｋが情報処理装置１０１ｂへと転送されて、ＩＣカード１０３ｂ側で実行される処理は終了する。

【００９７】さて、情報処理装置１０１ｂのＩＣカード１０３ｂ用のＩ／Ｏポート２０２ｂが、ＩＣカード１０３ｂ側から転送されたデータ暗号化鍵Ｋを受付けると、情報処理装置１０１ｂ側では、このデータ暗号化鍵Ｋが一旦メモリ２０５ｂに格納された後、以下に示すデジタル署名の確認処理が開始される。

【００９８】まず、ＤＥＳ暗号処理部２０４ｂおいて、電子メールに含まれるメールデータＰの暗号文Ｃが復号される。すなわち、ＤＥＳ暗号処理部２０４ｂおいて、メモリ２０５ｂに格納されたデータ暗号化鍵Ｋを使用した、次式に基づく復号処理が実行される。

【００９９】
【数３２】
$$P = D\ (K : C) \quad \cdots 数式３２$$
【０１００】そして、デジタル署名検証部２０９ｂにおいて、電子メールに含まれるデジタル署名$sgn_1(P)$と、ハッシュ計算部２０８ｂにおいて作成されるデータ$f(z(P,Ia,Ib,T))$とが、次式の関係を満足するこ

$$f\ (z\ (Ia,\ Ib,\ P,\ T)) \equiv sgn_1\ (P)^{e_1} \pmod{n_1} \quad \cdots 数式３３$$

【０１０２】この関係を満足すれば、その電子メールの機密性は保たれていることを意味し、反対にこの関係を満足しないならば、何者かによって不当にメールデータＰの内容が改竄されていることを疑う必要がある。
【０１０３】本実施例に係るシステムでは、このように、電子メールの送信元Ａにおいて、メールデータＰ、電子メールの送信元Ａを識別するためのユーザ情報Ｉａ、電子メールの送信先Ｂを識別するためのユーザ情報、電子メールの送信日時を特定するための時間情報Ｔを含めた送信データに対してデジタル署名が付与されるため、電子メールの受信側において、電子メールの送信元の検証、電子メールの宛先の検証、電子メールの作成日時の検証を行なうことができる。従って、従来技術の欄で説明したＰＥＭの管理下では起こり得た、不正なユーザによるメールデータの内容のすり替え等を防止することができる。すなわち、本実施例に係るシステムによれば、従来技術の欄で説明したＰＥＭよりも多岐に渡って電子メールの機密性を保持することができる。また、認証局の公開鍵(ｅ', ｎ')及びユーザの秘密鍵ｄの暗号に係る処理をＩＣカード内部のみで行なうため、これを所持する正当なユーザ以外の者に対する認証局の公開鍵(ｅ', ｎ')の機密性が保証され、かつ、自身以外のユーザに対する秘密鍵の機密性が保持される。従い、システム全体としての安全性が向上する。
【０１０４】ところで、本実施例に係るシステムでは、認証局の公開鍵(ｅ', ｎ')及びユーザの秘密鍵ｄの機密性を保証するためＩＣカードを使用しているが、必ずしもこれを使用する必要はない。例えば、ＰＥＭと同様な公開鍵証明書等を使用しても構わない。ただし、この場合には、認証局の公開鍵(ｅ', ｎ')及びユーザの秘密鍵ｄの正当性が確保されるように公開鍵証明書等の配布が充分慎重に行なわれる必要があり、更に、図５に示すように、本システムを構築する情報処理装置には、図３のＩＣカードが備える鍵暗号生成部３０２と同様な処理を行なう鍵暗号生成部５０７を新たに付加する必要がある。その代わり、ＩＣカード用のＩ／Ｏポートは不要となる。なお、こうした場合には、ＩＣカードのメモリの代用として、自身の秘密鍵d_1の暗号文C_1と認証局の公開鍵(ｅ', ｎ')とを格納したフロッピディスク等の記憶媒体を利用するようにしても良い。
とが確認される。ただし、Ｐは、ＤＥＳ暗号処理部２０４ｂで得られたメールデータであり、Ｉａは、電子メールの送信元Ａのユーザ情報であり、Ｉｂは、自身Ｂのユーザ情報であり、Ｔは、電子メールのヘッダに含まれる送信日時を特定する時間情報である。
【０１０１】
【数３３】
【０１０５】これまで電子メールの送信元と送信先が１対１の場合を例として説明してきたが、電子メールの送信形態には、送信元Ａが、同一内容のメールデータを含む電子メールを、複数の送信先$B_1,..,Bn$に対して同時に送信するというものがある。本実施例に係るシステム下で、こうした電子メールの送信形態をとる場合には、送信元Ａにおいて送信データｍを作成する際に、ハッシュ関数ｆに入力データを与える連接関数ｚの入力データとして、送信元Ａのユーザ情報Ｉａと、全複数の送信先$B_1,..,Bn$のユーザ情報$Ib_1,..,Ibn$と、メールデータＰと、現在の日時を特定する時間情報Ｔとを与えれば良い（次式参照）。
【０１０６】
【数３４】
$$m = f\ (P) \quad \cdots 数式３４$$
【０１０７】最後に、本システムとＰＥＭをまたがった電子メールの送受信について説明しておく。こうした場合には、電子メールを送受信するユーザ同士が、互いに、相手の利用するシステムを認識している必要がある。従って、ユーザは、システムへの登録を依頼する際に、自身が利用する電子メールの暗号化方式を特定するための情報（例えば、電子メールの暗号化方式の名称）を含んだ固有情報を送信するようにする。一方、ＰＥＭにおいては、認証局は、ユーザが利用する電子メールの暗号化方式を特定するための情報（例えば、ＰＥＭ等の、電子メールの暗号化方式の名称）を含んだ情報を暗号化した暗号文を記載した公開鍵証明書を発行する。
【０１０８】さて、本システムの側において、このようにシステムをまたいで相互に電子メールを送受信する場合に対応するためには、数式２５及び数式３３の連接関数ｚを、次式を満たすように定めておく必要がある。
【０１０９】
【数３５】
$$z\ (P) = P \quad \cdots 数式３５$$
【０１１０】そして、本システムを利用するユーザから、ＰＥＭを利用するユーザへと電子メールを送信する場合には、次式に基づいて送信データｍを作成すればよい。
【０１１１】
【数３６】

21

$$m = f(z(P)) \quad \cdots \text{数式３６}$$

【０１１２】一方、本システムを利用するユーザが、ＰＥＭを利用するユーザからの電子メールを受信した場合には、次式に基づいて、デジタル署名の確認処理を行えばよい。

22

【０１１３】

【数３７】

$$f(z(P)) \equiv sgn_1(P)^{e_1} \pmod{n_1} \quad \cdots \text{数式３７}$$

【０１１４】

【発明の効果】本発明に係る電子メールシステムによれば、電子メールの送受信に関するセキュリティの向上を図ることができる。

【図面の簡単な説明】

【図１】本発明の実施例に係るシステム構成の一例を説明する図である。

【図２】図１の情報処理装置の機能的な構成を説明する図である。

【図３】図１のＩＣカードの機能的な構成を説明する図である。

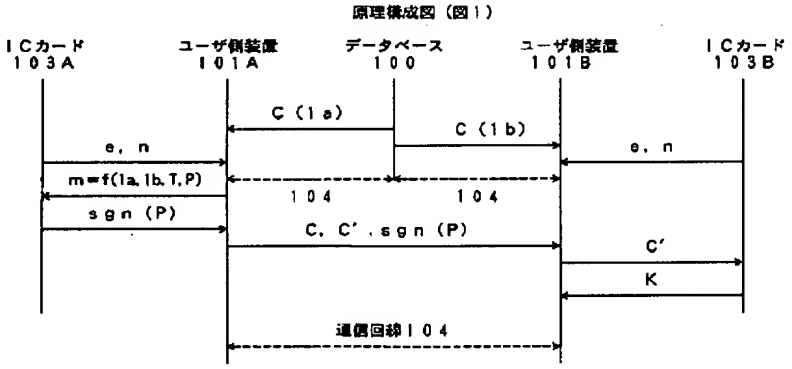
【図４】本発明の実施例に係るシステムを構成する情報処理装置の機能的な構成の一例を説明する図である。

【図５】本発明の実施例に係るシステムを構成する情報処理装置の機能的な構成の他の一例を説明する図である。

【符号の説明】

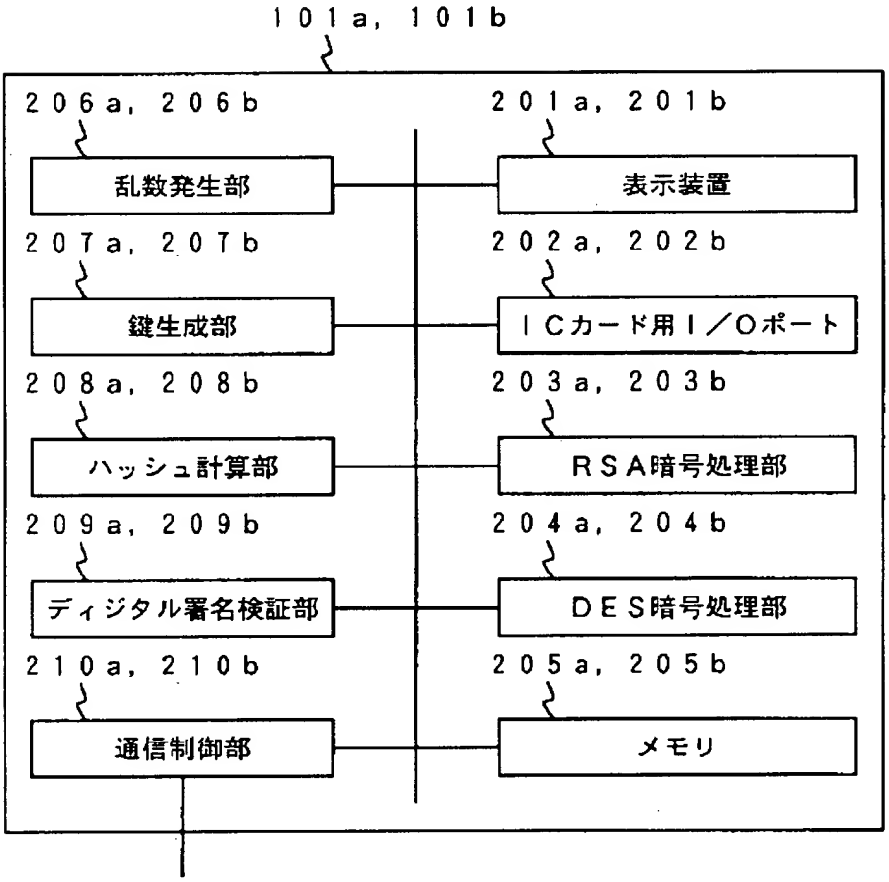
１００，１０１ａ，１０１ｂ…情報処理装置
１０３ａ，１０３ｂ…ＩＣカード
１０４…通信回線
２０１ａ，２０１ｂ…表示装置
２０２ａ，２０２ｂ…ＩＣカード用のＩ／Ｏポート
２０３ａ，２０３ｂ…ＲＳＡ暗号処理部
２０４ａ，２０４ｂ…ＤＥＳ暗号処理部
２０５ａ，２０５ｂ…メモリ
２０６ａ，２０６ｂ…乱数発生部
２０７ａ，２０７ｂ…鍵生成部
２０８ａ，２０８ｂ…ハッシュ計算部
２０９ａ，２０９ｂ…デジタル署名検証部
２１０ａ，２１０ｂ…通信制御部
２１２…バス
３０１ａ，３０１ｂ…入力部
３０２ａ，３０２ｂ…鍵暗号生成部
３０３ａ，３０２ｂ…メモリ
３０４ａ，３０４ｂ…ＤＥＳ暗号処理部
３０５ａ，３０５ｂ…ＲＳＡ暗号処理部
３０６ａ，３０６ｂ…デジタル署名作成部
３０７ａ，３０７ｂ…出力部

【図１】



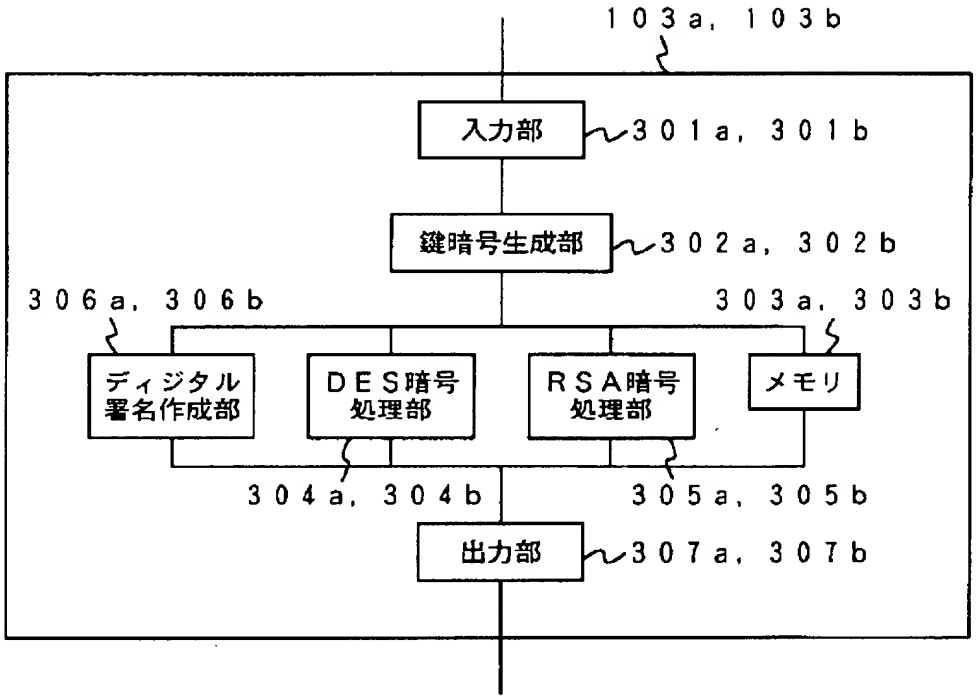
【図２】

ユーザ側装置内部構成（図２）



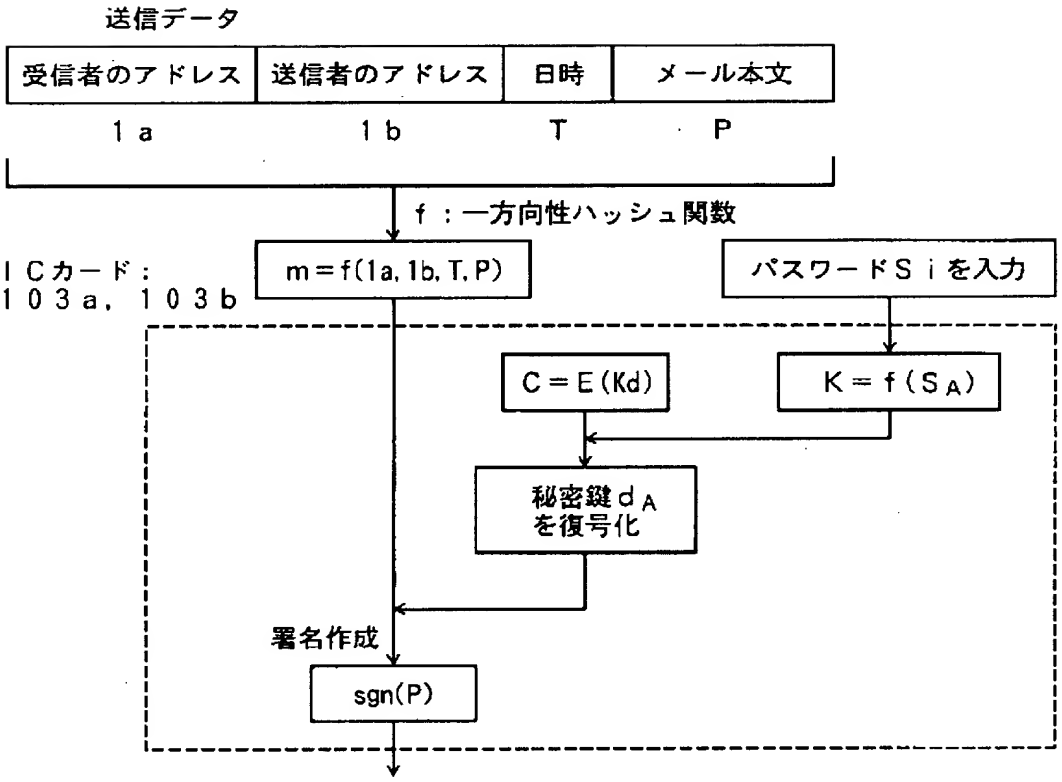
【図３】

ＩＣカード内部構成（図３）



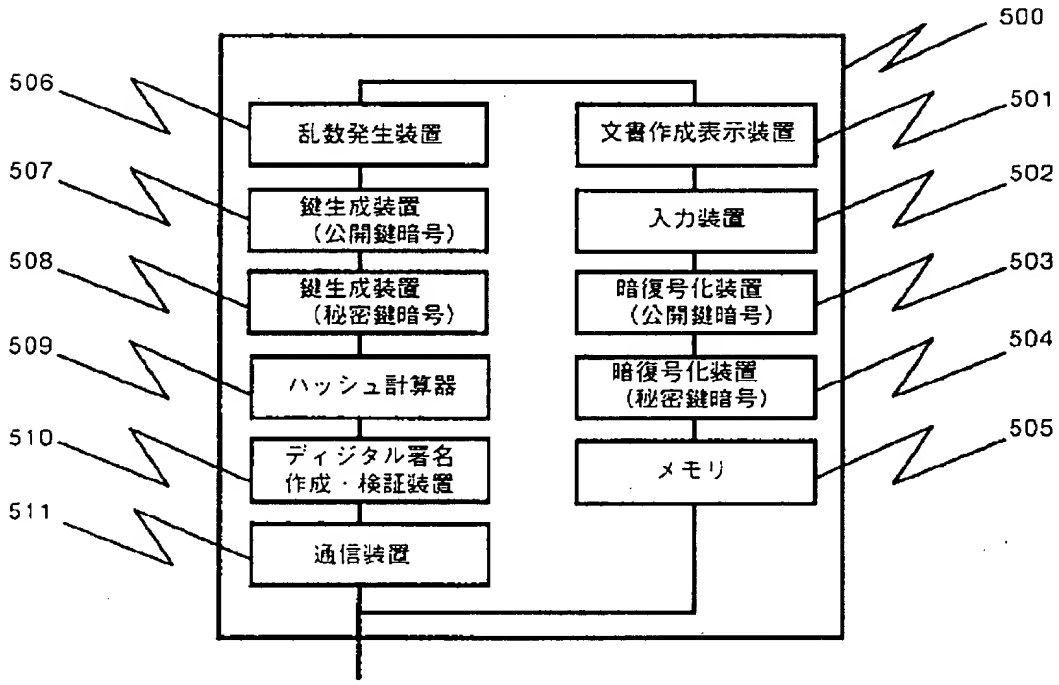
【図４】

署名作成手順（図４）


送信データ
受信者のアドレス
送信者のアドレス
日時
メール本文
1a
1b
T
P
f：一方向性ハッシュ関数
ICカード：
103a，103b
m＝f(1a,1b,T,P)
パスワードSiを入力
C＝E(Kd)
K＝f(SA)
秘密鍵dA
を復号化
署名作成
sgn(P)

【図５】

ユーザ側装置内部構成（図５）



フロントページの続き

(51) Int. Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
H04L	9/32			H04L	9/00	673E
	12/54					675A
	12/58		9466－5K		11/20	101B